Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Horizontal Internal Audit of Business Continuity Planning (BCP) in Large and Small Departments

Published: 2018-08-17

© Her Majesty the Queen in Right of Canada,
represented by the President of the Treasury Board, 2018

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-44/2018E-PDF
ISBN: 978-0-660-27228-3

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Audit interne horizontal de la planification de la continuité des activités (PCA) dans les grands et les petits ministères

Government of Canada | Gouvernement du Canada

Horizontal Internal Audit of Business Continuity Planning (BCP) in Large and Small Departments

From Treasury Board of Canada Secretariat

Notice to readers

This report contains either personal or confidential information, or information related to security, which has been withheld in accordance with the Access to Information Act.

October 2017
Office of the Comptroller General

On this page

- Executive summary
- Conformance with professional standards
- Background
- Detailed findings and recommendations
- Conclusion
- Management response
- Appendix A: Applicable policies, directives, standards, guidance, and best practices
- Appendix B: Departments included in the audit
- Appendix C: Lines of enquiry and audit criteria
- Appendix D: Recommendations by department and risk ranking
- Appendix E: Additional background on emergency management
- Appendix F: Roles and responsibilities of the main lead security agencies and central agency

Executive summary

In this section

- Why this is important
- Key findings
- Conclusion

The objectives of this audit consisted in determining whether the following were in place [1]:

- government-wide and departmental governance frameworks for business continuity planning (BCP)
- departmental BCP processes

The audit scope focused on frameworks and processes in place as at December 31, 2015. Emergency management as a broader topic, Information Technology (IT) continuity planning [2], and continuity of constitutional government [3] were excluded from the audit scope given their unique nature, complexities, and risks.

Why this is important

Globally, natural and man-made disasters are on the rise and have become key challenges. For instance, over the past seven years, environment-related risks (e.g. extreme weather events) have consistently featured among the top-ranked global risks identified by the World Economic Forum [4]. In 2017, terrorism was added to this list of top global risks. A similar trend is also prevailing in Canada.

Federal government operations are therefore now more likely than ever before to be disrupted by man-made and natural events. A disruption in the availability or integrity of some federal government services could result in a high degree of injury to the health, safety, security, and economic well-being of Canadians, or to the effective functioning of government as a whole (these services are hereafter referred to as "critical services"). [5] Similar disruptions in other types of services could also prevent individual federal government departments from being able to continue fulfilling their important mandates to Canadians (for the purpose of this audit, these services are hereafter referred to as "mission critical services"). Although some critical and mission critical services may be more obviously identified since the previously mentioned impacts would occur almost instantaneously following a disruption, this is not always the case. Other non-critical services may also become critical and/or mission critical if they are not fully restored within a specific extended period of time after a disruption.

There is also currently a greater risk that even localized disruptions in one or a few federal departments could have widespread repercussions across government operations, given the interdependencies that now exist between departments as a result of the growing adoption of shared service delivery models.

Strongly integrated BCP governance and processes are therefore key to enhancing the resilience [6] of government operations and service delivery. More specifically, in the event of disruptions to normal government business operations, these elements will help enable the continuation of service delivery to Canadians with minimal or no downtime.

Key findings

Governance frameworks over BCP

The audit examined whether governance frameworks over BCP were in place at the government-wide and departmental levels. Overall, the audit found that elements of such frameworks were in place but need significant improvements at both levels.

The audit noted that government-wide policy direction for BCP was established by the Treasury Board security policy framework, with more up-to-date guidance recently provided in certain areas by Public Safety Canada, as a lead security agency responsible for providing leadership in the area of emergency management (which includes continuity of operations). However, foundational policy instruments have not been updated in many years, and in several cases, their accessibility was limited. BCP program policies were established in most large departments but generally were not in small departments. In departments where such policies were in place, many had not been updated in several years. An opportunity to strengthen the communication of BCP roles and responsibilities to stakeholders was also noted in most departments.

In support of security and emergency management governance, several interdepartmental committees were established and addressed matters relating to BCP across government. The audit also noted that similar governance committees were in place within most departments. However, both government-wide and departmental committees generally did not demonstrate having actively supported BCP by meeting regularly, and systematically tracking as well as following-up on initiatives in this regard.

Core emergency management strategic themes were developed at the government-wide level and identified the need to strengthen emergency management planning, including BCP, as one of the federal strategic priorities. At the time of the audit, however, an integrated strategy outlining how BCP is to be strengthened across government and how initiatives in this regard will be coordinated had not yet been developed.

Furthermore, the audit noted that although governance committees established under the Federal Emergency Response Plan (FERP) are in place to coordinate a federal response in the event of an interdepartmental disruption (from a continuity of government operations standpoint), a more proactive and centralized coordinated approach could help ensure the availability as well as maintenance of reliable and timely information from departments about the critical services they deliver. Improvements in the quality and availability of information in this area would help better inform decision-making when a federal response is required.

Finally, the audit noted that there was limited monitoring and reporting of BCP across government. At the government-wide level, monitoring of BCP mostly relied on Management Accountability Framework (MAF) assessments of compliance with BCP program requirements established by the Treasury Board of Canada Secretariat (the Secretariat). Conversely, departments generally did not demonstrate having monitored the overall compliance and effectiveness of their BCP programs. Additionally, none of the departments demonstrated having put in place both a comprehensive and formal approach to regularly test as well as validate the business continuity plans examined as part of this audit.

Departmental processes for BCP

As part of baseline security requirements, all departments must have business continuity plans in place to provide for the continuity of government operations, regardless of whether they deliver critical services or not. Conducting a Business Impact Analysis (BIA) constitutes a fundamental starting point in the process for developing such plans. The Operational Security Standard – Business Continuity Planning (BCP) Program outlines various other activities that must be conducted as part of this process, including requirements for the content of BIAs and business continuity plans.

The audit assessed a risk-based sample of BIAs and departmental business continuity plans to determine the extent to which departments complied with these requirements.

Although the majority of departments conducted BIAs and had business continuity plans in place for all services sampled, significant opportunities for improvements were noted regarding their content and the process carried out for developing them. More specifically, departments generally have not met most of the baseline requirements prescribed by the Secretariat for BIAs, and baseline requirements for business continuity plans were mostly not met for many departmental plans examined.

Conclusion

Overall, the audit noted a significant need for improvements to the departmental and government-wide governance frameworks as well as to the BCP processes in place within departments.

At the government-wide level, opportunities for improvements to BCP governance were noted in the following areas: accessibility and updating of policy instruments; strengthening support from senior interdepartmental governance committees; strategic planning; [This information has been withheld] and, monitoring and reporting frameworks.

Within departments, there is also a need to improve governance over BCP through more active support from governance committees, better communication of roles and responsibilities, and stronger monitoring and reporting frameworks (including testing of business continuity plans).

Finally, the alignment of departmental BCP processes with baseline requirements is also an area that needs improvement.

Conformance with professional standards

This audit engagement was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.

Mike Milito, MBA, CIA, CRMA
Assistant Comptroller General and Chief Audit Executive
Internal Audit Sector, Office of the Comptroller General

Background

In this section

- Audit objectives and scope

Business continuity planning (BCP) is a proactive security measure to help increase organizations' resilience to disruptive events. More specifically, BCP refers to the development and timely execution of plans, measures, procedures, and arrangements to ensure minimal or no interruption to the availability of services and assets when a disruption to normal business operations occurs, regardless of the disruption's origin. BCP is therefore key to the survival of organizations. On a broader scale, BCP complements emergency management because it supports preparedness, response, and recovery activities.

The ultimate purpose of emergency management is to save lives, preserve the environment, and protect property and the economy. Emergency management raises the understanding of risks and contributes to a safer, more prosperous, sustainable, and disaster resilient society in

Canada. Emergency management in federal, provincial, and territorial governments adopts a comprehensive all-hazards approach [7] to coordinate and integrate the prevention and mitigation, preparedness, response, and recovery activities to maximize the safety of Canadians (refer to Appendix E for additional background on Emergency Management).

As per the federal Emergency Management Act, the emergency management responsibilities of each deputy head consist of identifying the risks that lie within the purview of their department, and in:

- preparing emergency management plans (for example, strategic emergency management plan, building emergency evacuation plans, etc.) addressing these risks
- maintaining, testing, and implementing those plans
- conducting exercises and training in relation to those plans

Under the Emergency Management Act departmental emergency management plans are required to be supported by "programs, arrangements or other measures to provide for the continuity of the operations." Such support is achieved by establishing departmental BCP programs that comprise the following: [8]

- BCP Program governance (for example, BCP policy, appointment of a BCP coordinator, etc.)
- business impact analysis (BIA) [9]
- business continuity plans and arrangements [10]
- maintenance of BCP Program readiness (for example, review and revision of all plans, regular testing, etc.)

Although responsibility for departmental BCP programs rests with deputy heads, ensuring the continuity of government operations as a whole is a shared responsibility among several stakeholders (central agency, lead security agencies and departments).

Lead security agencies are responsible for providing advice, guidance, and services to support the day-to-day security operations of departments and for enabling the government as a whole to: manage security activities, coordinate responses to security incidents, and achieve and maintain an acceptable state of security and readiness.

The main lead security agencies responsible for enabling the continuity of government operations as a whole are (see Appendix F for further details):

- the Treasury Board and its Secretariat for their policy roles as a central agency
- Public Safety Canada for its leadership role in emergency management and BCP
- the Privy Council Office for its national security role

The Treasury Board security policy framework, which provides direction on BCP within government, aims to ensure that deputy heads effectively manage security activities within departments while also contributing towards effective management of government-wide security.

The policy framework is comprised of the following instruments (see Appendix A):

- the Treasury Board's Policy on Government Security
- the Secretariat's Directive on Departmental Security Management
- the Secretariat's Operational Security Standard - Business Continuity Planning (BCP) Program
- technical BCP program guidance issued by Public Safety Canada

Because most of these policy instruments came into effect in or before 2009, the Secretariat and Public Safety Canada are in the process of renewing them to better reflect the federal government's current strategic and operating environment.

During consultations for the Office of the Comptroller General's Three-Year Risk-Based Internal Audit Plan 2015-18, specific concerns were raised about BCP. These concerns related to challenges such as: the increased interdependencies that now exist between departments as a result of the transition towards shared service delivery models; the complexity of BCP itself; and, the risk that departmental business continuity plans may not have been updated in a timely manner over the years.

Audit objectives and scope

The objectives of this audit were to determine whether the following were in place [11]:

- government-wide and departmental governance frameworks for BCP
- departmental BCP processes

The scope of the audit focused on practices in place as at December 31, 2015. A risk-based sample [12] of departmental business continuity plans in place as of this date was examined to assess departmental BCP processes. Governance frameworks and BCP processes were expected to align with policy requirements (see Appendix A). In order to better present findings and recommendations in the current context, initiatives undertaken subsequent to December 31, 2015, and observed during the audit fieldwork were also considered.

The elements of governance examined were as follows: policy frameworks; committees and organizational structures; strategic planning at the government-wide level; [This information has been withheld]; interdepartmental collaboration processes; as well as, monitoring and reporting.

The elements of BCP processes examined were as follows: BIA; development of recovery strategies; development of business continuity plans; management of interdependencies with internal and external stakeholders; BCP training and tools; monitoring as well as reporting (including testing); and, maintenance of business continuity plans.

The audit focused solely on the departmental and government-wide BCP practices in place to ensure the continued availability of federal government services (both critical services and mission critical services). The following were excluded from the audit scope given their unique nature, complexities, and risks: emergency management as a broader topic; Information Technology (IT) continuity planning [13]; and, continuity of constitutional government [14].

Appendix B lists the departments and lead security agencies included in the audit.

Appendix C outlines the lines of enquiry and related audit criteria used to conclude on the audit objectives.

Detailed findings and recommendations

In this section

- Finding 1: Governance at the government-wide level
- Finding 2: Governance at the departmental level
- Finding 3: Departmental BCP processes

Finding 1: Governance at the government-wide level

Having governance structures in place at the government-wide level is one of the expected results of the Treasury Board Policy on Government Security. Under this policy, deputy heads are accountable for effective security governance [15] within their departments. They also share responsibility for the security of government as a whole. Lead security agencies share responsibility for supporting departments by providing advice, guidance and services to support the day-to-day security operations of departments and enable government as a whole to effectively manage security activities, coordinate response to security incidents, and achieve as well as maintain an acceptable state of security readiness.

Given the large size and complexity of federal government operations, the various stakeholders involved, and the interdependencies between departments, having clearly defined government-wide governance is key to effectively coordinate efforts to ensure the continuity of federal government operations.

The audit examined whether lead security agencies and departments carried out their BCP governance responsibilities under the Emergency Management Act, the Financial Administration Act, the Federal Policy on Emergency Management, the Policy on Government Security, the Directive on Departmental Security Management, and the Operational Security Standard – Business Continuity Planning (BCP) Program. At the government-wide level, the audit focused on the following aspects of governance over continuity of government operations and services: policy instruments, whole-of-government committee structures, strategic planning of initiatives supporting departments, government-wide monitoring and reporting frameworks as well as [This information has been withheld]

Policy instruments were not all readily accessible, and in most cases have not been updated in several years. Work is in progress to renew policy instruments, and more recent technical guidance was issued in certain areas.

The Secretariat and Public Safety Canada have overlapping responsibilities for providing direction to departments on BCP (see Appendix F). Consequently, both were expected to coordinate their efforts to ensure that their responsibilities were addressed and that their respective policy instruments are consistent.

Pursuant to its mandated responsibilities, the Secretariat has published policy instruments on its website to support a whole-of-government approach to BCP. The Secretariat provided government-wide direction on roles, responsibilities and expectations in this area mainly through the following: the Policy on Government Security, the Directive on Departmental Security Management, and, the Operational Security Standard - Business Continuity Planning (BCP) Program. However, these foundational policy instruments have not been updated in several years (for close to a decade in most cases), and the Secretariat has repeatedly postponed its targeted timelines for doing so. Over the years, significant changes have occurred in the government's operational environment. The growing adoption of shared service delivery models is an example. Secretariat representatives explained that delays in updating the government's security policy suite resulted from a need to undertake more detailed analysis to further increase the clarity of requirements.

The Secretariat demonstrated that it was actively working at renewing the government's security policy instruments in consultation with Public Safety Canada, and a variety of interdepartmental committees. For instance, draft versions of the renewed Policy on Government Security and Directive on Security Management that resulted from interdepartmental consultations led by the Secretariat were presented for endorsement at the Public Service Management Advisory Committee meeting in September 2016 and were published on the federal government's intranet (GCpedia).

In alignment with its mandated responsibilities under the Emergency Management Act, Public Safety Canada issued A Guide to Business Continuity Planning, which is readily accessible on its public Internet website. This publication provides high-level guidance on BCP for all types

of organizations in the private and public sectors. Although Public Safety Canada has developed several other technical guides and tools to provide more specific guidance on BCP within the federal government, these resources were not as readily available as the previously mentioned Public Safety Canada guide. The audit also noted that many of these resources have not been updated in several years and that some referred to policy instruments that the Secretariat rescinded many years ago.

During the audit fieldwork, Public Safety Canada demonstrated that it had begun to update its resources supporting government-wide BCP. It also provided the audit team with an internal work plan that outlined several initiatives to enhance BCP support to departments in areas such as: program development, training, advisory services, outreach, and communications. For example, in 2016, Public Safety Canada developed A Guide for Developing a Business Continuity Management Program for Small Departments and Agencies. In developing this guide, Public Safety Canada consulted a subset of representatives from the community of small departments, including the Secretariat's policy centre. Although no evidence was provided to demonstrate that the guide was subsequently communicated to all small departments across government, the evidence examined demonstrated that it was communicated via email to participants of the Security Advisory Network for Small Agencies.

Nevertheless, only a few large departments included in this audit indicated that their needs were met in terms of BCP guidance from lead security agencies (the Secretariat, in its central agency role, and Public Safety Canada). In small departments, the majority of representatives interviewed indicated that the guidance provided by lead security agencies on BCP has not met their needs. Representatives in both large and small departments indicated that their concerns included the following: guidance is not readily accessible; lack of clarity in terminology; and, the guidance available is too broad as well as outdated. Several representatives of small departments also indicated that they were not aware of Public Safety Canada's A Guide for Developing a Business Continuity Management Program for Small Departments and Agencies.

Having up-to-date government-wide BCP policy instruments that are broadly communicated, harmonized, and that reflect the current government operating environment, could reduce the risk that roles, responsibilities, expectations and requirements are not clearly understood and implemented. This in turn could contribute to increasing the federal government's readiness and resilience to disruptions.

Government-wide senior management committees were established to oversee broader areas related to BCP (emergency management and government security). However, there was limited indication that these committees were actively involved in addressing matters specific to BCP.

Senior management commitment to BCP is essential and to achieve a high level of resiliency, efforts must be concerted across the federal government. Public Safety Canada and the Secretariat share the main responsibilities in this regard at the government-wide level (see Appendix F).

Collectively, the Secretariat and Public Safety Canada established several interdepartmental senior management committees in addition to working groups and forums to support a whole-of-government approach to security as well as emergency management. Although the government-wide senior management committees have indirectly demonstrated their support to BCP when addressing matters related to broader initiatives (such as the Treasury Board's policy suite reset and core strategic themes for federal emergency management), there was limited evidence demonstrating their support for BCP specifically. The audit also noted that there was limited representation of small departments on these government-wide senior management committees.

At the working level, Public Safety Canada established informal governance groups that specifically address BCP. For instance, in September 2015, the establishment of a federal Emergency Management/Business Continuity Community of Practice was approved to promote best practices and the exchange of information between departments. In the same month, Public Safety Canada held separate interdepartmental working group meetings with representatives of small departments and the Secretariat to develop its Guide for Developing a Business Continuity Management Program for Small Departments and Agencies, which was finalized in 2016. Public Safety Canada subsequently held an interdepartmental session to obtain feedback on emergency management and BCP tools for small departments and agencies in November 2015.

The Privy Council Office established informal governance committees (for example, the Departmental Security Officer Readiness Committee and its cluster groups) and a center for development with broad security mandates that encompass BCP to support the Departmental Security Officer community in fulfilling its duties at the working level.

Active and direct involvement from relevant senior interdepartmental management committees related to security and emergency management, and better representation of small departments at these committees, would raise the profile of BCP across government. In turn, this would help ensure that BCP receives due consideration as part of decision making in all departments, such as when establishing priorities and in making decisions about allocating resources.

There is a lack of strategic planning at the government-wide level regarding BCP. Work is in progress to develop federal emergency management strategic priorities that encompass BCP.

The Treasury Board Policy on Government Security recognizes the need to establish a whole-of-government security approach to support departments and enable government in order to effectively manage security as well as achieve and maintain an acceptable state of readiness. The Policy states that "security is achieved when it is supported by senior management – an integral component of strategic and operational planning – and embedded into departmental frameworks, culture, day-to-day operations and employee behaviours." It also states that "at a government-wide level, security threats, risks and incidents must be proactively managed to help protect the government's critical assets, information and service, as well as national security". Because BCP is considered a baseline security requirement, we expected a risk-based government-wide level strategy that encompasses BCP to be in place.

According to the Policy on Government Security, the Secretariat is responsible for exercising strategic oversight, providing leadership, and establishing priorities related to government security. Because Public Safety Canada is the federal coordinating department responsible for exercising leadership in emergency management under the Emergency Management Act, both the Secretariat and Public Safety Canada share responsibility for strategic planning at the government-wide level regarding BCP.

Pursuant to its mandated leadership responsibilities, Public Safety Canada sought input from interdepartmental senior management committees to identify cross-cutting priorities across the federal emergency management community and help shape a shared strategic agenda.

Based on the input provided, Public Safety Canada subsequently led discussions in 2015 at these committees on an approach to increase interdepartmental collaboration and advance strategic priorities. As a member of these committees, the Secretariat participated in these discussions. A general consensus was reached on the proposed core emergency management strategic themes and about the need to develop a multi-year work plan to operationalize these themes. Interdepartmental assistant deputy minister committees and Public Safety Canada also raised the need to engage deputy ministers in this regard. Strengthening emergency management planning, including BCP, was identified as a priority under one of the core strategic themes.

Although work in this area is ongoing, the following three core emergency management strategic themes were identified to enable resilience within the current risk environment:

- capabilities and capacities: Enhancing capabilities and capacities include having the right structures, resources, and tools in place to deal with events and emergencies
- knowledge and innovation: Facilitating greater knowledge exchanges, research, and innovation will identify new opportunities and enable more integrated approaches
- relationships and culture: Relationships and culture enhance societal resilience by promoting risk awareness and building trust among a variety of diverse actors

At the time of the audit, however, a specific integrated strategy to strengthen BCP across government and a government-wide level action plan to implement such a strategy had not yet been developed. Deputy ministers also had not yet been engaged on the proposed core emergency management strategic themes.

Enhancing resilience within an evolving risk environment requires a more integrated approach. Through formal integrated strategic planning at a government-wide level, the Government of Canada should be able to increase its ability to achieve the expected results outlined in the Secretariat's security policy suite and effectively increase its resilience to disruptions by focusing resources in areas of higher risk.

Government-wide monitoring of BCP was limited. Work is in progress to further enhance monitoring and reporting frameworks.

Monitoring of BCP at the government-wide level is a shared responsibility between the Secretariat and Public Safety Canada. The Secretariat is responsible for monitoring government-wide compliance with the Treasury Board security policy suite and the achievement of its expected results. The Secretariat is also expected to have reviewed and reported to the Treasury Board on the effectiveness and implementation of this policy suite at the five-year mark from the effective date of the Policy on Government Security (by July 2014).

Under the Emergency Management Act, Public Safety Canada is responsible for "analysing and evaluating emergency management plans prepared by government institutions" including business continuity plans. Public Safety Canada's responsibilities pursuant to the act also include conducting exercises related to emergency management. In terms of reporting, there is a requirement in the Federal Policy for Emergency Management for Public Safety Canada to "report every two years to the Deputy Ministers' Committee responsible for emergency management issues on the implementation of this policy and on the government-wide readiness of the federal emergency management system, based on the information reported by federal institutions and work undertaken directly by Public Safety Canada."

Finally, as per the Policy on Government Security, both the Secretariat and Public Safety Canada are responsible to ensure "that periodic reviews are conducted to assess the effectiveness of their security support services to ensure they continue to meet the needs of departments and the government as a whole".

Through the conduct of Management Accountability Framework assessments in 2014-15 and in 2015-16, the Secretariat demonstrated that it has fulfilled its government-wide responsibility to monitor compliance with BCP policy requirements. The Secretariat also participated in ad hoc lessons learned exercises conducted jointly with other lead security agencies and departments after the occurrence of security incidents. However, the Secretariat did not meet the previously mentioned reporting requirement to the Treasury Board, and did not demonstrate that it has periodically assessed the effectiveness of its support initiatives with respect to BCP.

In alignment with its government-wide monitoring responsibility as a lead security agency under the Policy on Government Security, Public Safety Canada conducted interdepartmental working group meetings and feedback sessions with representatives of small departments to review and improve the BCP guidance as well as tools available to them. Regarding its legislative responsibility for conducting emergency management exercises, Public Safety Canada has fulfilled this responsibility by developing a multi-year National Exercise Schedule for 2013-16 and by conducting a national exercise in 2014 that covered BCP. An After Action Report for this exercise was prepared by Public Safety Canada and presented to the assistant deputy minister and director general emergency management committees.

Beyond these initiatives, Public Safety Canada did not demonstrate that it has periodically assessed the effectiveness of its support initiatives with respect to BCP. Public Safety Canada also did not demonstrate that it has assessed the business continuity plans of other departments, and this issue was previously raised in both the 2009 Fall Report of the Auditor General of Canada and in the 2014 Public Safety Canada Internal Audit of Emergency Management Planning: Leadership & Oversight. Although the OAG did not issue any specific recommendation in its 2009 report to address this issue, a recommendation in this area was issued in the aforementioned Public Safety Canada's 2014 internal audit report.

Furthermore, we noted that Public Safety Canada has not fulfilled its responsibility to report on government-wide readiness with respect to continuity of government operations. The 2014 Public Safety Canada Internal Audit of Emergency Management Planning: Leadership & Oversight concluded that overall, Public Safety Canada "does not have sufficient or effective mechanisms to appropriately gauge the readiness of federal institutions in the face of emergencies. As well, lack of monitoring limits the Department's ability to gain insight into the strengths and challenges within federal institutions which itself should inform Public Safety Canada directions, policy and guidance."

During the audit fieldwork, evidence was provided demonstrating that the Secretariat and Public Safety Canada are actively working together to develop joint approaches in order to further enhance government-wide BCP monitoring and reporting frameworks.

Periodic monitoring of BCP at the government-wide level, and regular reporting of the results to interdepartmental senior management committees would help identify and address vulnerabilities more proactively as well as systemically across government. In turn, this would increase the government's resilience to disruptions.

At the government-wide level, the approach for [This information has been withheld] is reactive and relies on unverified assumptions. Work is in progress to adopt a more proactive approach in this regard.

Enhancing the government's resilience to disruptions within an evolving risk environment where interdependencies between departments have grown significantly requires a proactive and holistic approach to BCP. In terms of process, identifying and prioritizing critical services is

a fundamental starting point from a risk perspective. A compromise in the availability or integrity of these services would result in a high degree of injury to the health, safety, security, or economic well-being of Canadians, or to the effective functioning of the Government of Canada.

According to the Operational Security Standard - Business Continuity Planning (BCP) Program, departments are required to "conduct a business impact analysis to assess the impact of disruptions on the department and to identify and prioritize critical services and associated assets." The standard also prescribes a basic approach departments must follow when completing a BIA. [16] Furthermore, the Directive on Departmental Security Management has a requirement at the departmental level stating that "an up-to-date inventory of critical services and associated information, assets and dependencies is maintained and provided to Public Safety Canada as requested".

[This information has been withheld] Considering Public Safety Canada's leadership role as the federal coordinating department for emergency management and the Secretariat's role as a central agency for establishing and overseeing a government security policy, we expected both departments to have worked collaboratively in elaborating and implementing such an approach.

In January 2011, Public Safety Canada developed a Federal Emergency Response Plan (FERP) that outlined the Government of Canada's "all hazards" [17] response plan. The FERP outlines high-level processes and mechanisms to facilitate an integrated Government of Canada response to an emergency, and to eliminate the need for federal government institutions to coordinate a wider Government of Canada response. Annex A of the FERP provides a broad overview of the functions within government that are most frequently used in the context of a federal response to an emergency (emergency support functions). The Annex also identifies the departments with a primary and support role in each of these areas, including a general description of their responsibilities. According to the FERP, "during an integrated Government of Canada response, all involved federal government institutions assist in determining overall objectives, contribute to joint plans, and maximize the use of all available resources. This occurs at the national and regional levels as necessary, based on the scope and nature of the emergency". An extensive interdepartmental governance structure was also developed in support of the FERP to coordinate emergency management during non-emergency and emergency circumstances. [18]

Although the FERP provides an indication of which areas are typically key in a federal emergency response (that is, emergency support functions) and is supported by an extensive interdepartmental governance structure to coordinate emergency management activities, it does not explicitly outline [This information has been withheld] This is because the scope of the FERP is at a much broader emergency management level, and the intention of the FERP "is to employ generic methodologies, modified as necessary by particular circumstances."

Public Safety Canada representatives interviewed mentioned that critical services have "to varying extents" been identified by departments "based on their own authorities". Public Safety Canada representatives also added that "when a whole of government response is required (multiple departments are impacted by an event) and decisions are required [This information has been withheld] According to these representatives, such "decisions would be made by established FERP governance. BCP related decisions that do not impact an integrated Government of Canada response would remain internal to each department. As well, the FERP structure is focused on response activities and initial recovery only. The longer term activities which normally take place during the recovery phase are not dealt with under the FERP construct".

The approach at the government-wide level to [This information has been withheld] was therefore found to be reactive. Existing FERP governance structures are leveraged for this purpose only on an ad hoc basis, as emergencies that require an integrated government response arise. The approach at the government-wide level also relies on the ability of departments impacted by such emergencies to provide this information when needed. Considering there is limited monitoring of departmental BCP at the government-wide level, as indicated in the previous section, the audit concluded that at the government-wide level, the reactive approach also relies on unverified assumptions about the availability, timeliness, and accuracy of information from departments regarding critical services.

During the audit fieldwork, however, the audit team was provided with a draft [This information has been withheld] [19]

Finally, the audit noted that in 2016, representatives from both Public Safety Canada and the Secretariat held joint working-level meetings to clarify their respective roles and responsibilities as well as develop joint approaches for [This information has been withheld] The documentation developed as a result of these meetings outlined the value of [This information has been withheld] to support interdepartmental coordination and decision-making during a federal response as well as other emergency management activities. At the time of the audit, work in this area was still in progress, and Public Safety Canada representatives mentioned that "while ongoing discussions between Public Safety and the Treasury Board Secretariat have been taking place on this subject, there has been no formal agreement between the two parties on the development of a [This information has been withheld]

Adopting a more proactive approach at the government-wide level would contribute to increasing the quality of information about [This information has been withheld] in terms of availability, timeliness, and accuracy. In turn, this could also enhance the effectiveness and efficiency of BCP priority setting, related strategic decision-making, and event response from a government-wide perspective.

Governance frameworks at the government-wide level

BCP governance at the government-wide level is exercised mainly through policy instruments, interdepartmental governance committees, working groups, forums, and monitoring activities conducted as part of MAF assessments. The main departments involved in this regard are Public Safety Canada for its leadership role as the federal coordinating department, and the Secretariat for its policy role as a central agency.

Several opportunities for improvements were noted, including in the following areas: accessibility and updates to policy instruments; senior management support; strategic planning; monitoring and reporting; and, approach for the identification and prioritization of critical services.

Recommendations – Governance at the government-wide level

1. Public Safety Canada and the Secretariat should ensure that appropriate work plans to expedite the renewal of policy instruments that support BCP are in place and regularly monitored. In doing so, the Secretariat should also determine how to strengthen the linkages to Public Safety Canada's technical guidance on BCP within the renewed Treasury Board security policy framework.
2. Public Safety Canada should ensure that its technical guidance on BCP is communicated and made readily accessible to all departments.
3. Public Safety Canada and the Secretariat should periodically raise the profile of BCP in the agendas of interdepartmental senior management committee meetings related to security and emergency management. Representation of small departments at these committees should also be strengthened.
4. Public Safety Canada should, in consultation with the Secretariat, develop and implement a formal monitoring and reporting framework for periodically assessing the business continuity plans of other departments.
5. The Secretariat, with Public Safety Canada and the Privy Council Office, should establish a results-based government-wide strategy to strengthen the continuity of government operations and support federal departments in strengthening their BCP programs. The strategy should:
    a. address the specific needs of departments (for example, via practical hands-on training, tools, technical guidance, capacity development activities, targeted support where required, etc.)
    b. include the development of a proactive approach for enabling departments to provide timely and accurate BCP information, [This information has been withheld]
    c. be developed in consultation with the relevant senior interdepartmental security and emergency management committees, and specify the contributions of these committees for strengthening BCP government-wide
    d. be regularly monitored by the Secretariat, with Public Safety Canada, to help ensure the achievement of targeted results

e. take into consideration the results of all government-wide monitoring activities relating to BCP (for example, MAF assessments conducted by the Secretariat, evaluations of departmental business continuity plans conducted by Public Safety Canada, maturity assessments, etc.)

Finding 2: governance at the departmental level

The Treasury Board Policy on Government Security states that deputy heads are accountable for the effective implementation and governance of security within their departments, and that they share responsibility for security of government as a whole.

The audit examined whether departments carried out their governance-related responsibilities according to the Policy on Government Security, the Directive on Departmental Security Management, and the Operational Security Standard - Business Continuity Planning (BCP) Program. The audit focused on the following aspects of departmental governance for BCP: governance committees, communication of roles and responsibilities, testing, monitoring, and reporting.

Although the vast majority of departments have established governance committees to oversee and integrate BCP activities, most did not demonstrate that these committees were actively involved in this area.

As per the Policy on Government Security, "security is achieved when it is supported by senior management – an integral component of strategic and operational planning – and embedded into departmental frameworks, culture, day-to-day operations and employee behaviours." The Directive on Departmental Security Management requires departments to establish security governance mechanisms (such as committees and working groups) to ensure the coordination and integration of security activities and facilitate decision making. Governance is also identified as a key element of departmental BCP programs under the Operational Security Standard – Business Continuity Planning (BCP) Program. Departments were therefore expected to have governance committees in place that were actively involved in overseeing and integrating BCP activities.

The audit found that the vast majority of departments had formal senior management committees in place to oversee and support the coordination of their organizations' activities, including activities relating to BCP. The audit noted as a best practice that most large departments and some small departments had also established committees or working groups that had mandates specifically dedicated to BCP.

However, departments generally did not demonstrate that these governance committees actively supported BCP by meeting regularly (based on a pre-established frequency) and by systematically tracking as well as following-up on initiatives in this area.

Governance committees that actively demonstrate their support for BCP by meeting regularly and following-up on initiatives in this area would raise the profile of BCP. In turn, this would help ensure that the area will receive due consideration as part of the decision-making process and further enhance coordination between departmental stakeholders.

Communication of roles and responsibilities needs improvement in almost all departments.

The Operational Security Standard – Business Continuity Planning (BCP) Program states that an essential element of governance is the development of a departmental BCP Program policy approved by senior management to formally define and communicate expectations.

Departments also need to appoint a Departmental Security Officer (DSO) and BCP Coordinator. The Policy on Government Security indicates that the DSO is to be functionally responsible to the deputy head or to the departmental executive committee to manage the departmental security program. [20] The security responsibilities of the DSO include BCP, and the Operational Security Standard – Business Continuity Planning (BCP) Program requires that departments appoint a BCP Coordinator to support the DSO in this area. [21] Under this standard, the BCP Coordinator is expected to inform the DSO throughout the BCP process. [22]

The Directive on Departmental Security Management also requires departments to ensure that the accountabilities, delegations, reporting relationships, roles and responsibilities of departmental employees who have security responsibilities are defined, documented, and communicated to the relevant people. Departments were expected to have complied with these requirements for the BCP-related roles and responsibilities assigned to all employees involved in the departmental BCP process (for example, DSO, BCP Coordinator, functional managers, etc.) [23].

Although most of the large departments have demonstrated that BCP program policies approved by senior management were in place, this was generally not the case in small departments. The audit also noted that in half of the large departments where these policies were in place, the policies had not been updated in several years. Representatives in one of these large departments mentioned waiting for the Secretariat and Public Safety Canada to first update their related policy instruments.

The majority of departments have formally appointed a DSO and BCP Coordinator, in accordance with the requirements mentioned previously. The reporting relationship observed between these two stakeholders was also generally aligned with requirements. However, in half of the large departments, it was noted that the reporting relationship between the DSO and the deputy head (or executive committee) was not formally documented and communicated to both parties.

Regarding the communication of BCP roles and responsibilities to all employees involved in the departmental BCP process, opportunities for improvements were noted in most of the large departments, and in all of the small departments included in this audit. More specifically, most of the large departments did not demonstrate having formally communicated BCP-related roles and responsibilities to all employees involved in the BCP process. This was also found to be the case for all of the small departments examined. In several large and small departments, however, the audit did note that some employees were formally held accountable for their performance in fulfilling their BCP roles (for example, through their annual performance management agreement).

Ensuring that BCP-related roles and responsibilities are formally communicated to all individuals involved in the departmental BCP process would help foster a better understanding of expectations and the coordination of activities in this area. Additionally, formally holding all individuals accountable for their performance in fulfilling their respective roles and responsibilities as part of this process would further contribute to enhancing the overall effectiveness of the BCP program.

Departmental BCP monitoring and reporting frameworks were either non-existent or limited.

Under the government's security policy framework, departments are responsible for establishing monitoring and reporting frameworks to periodically assess the effectiveness and compliance of their BCP programs. The Operational Security Standard – Business Continuity Planning (BCP) Program also requires departments to conduct regular testing and validation of all their business continuity plans. [24]

Public Safety's A Guide to Business Continuity Planning recommends that all departments conduct internal reviews on an annual or bi-annual basis to ensure the accuracy, relevance and effectiveness of their business continuity plans. [25] Although issued subsequent to the audit period, Public Safety Canada's Guide for Developing a Business Continuity Management Program for Small Departments and Agencies (SDAs) recommends that "one walk through [26] or table top exercise [27] of the plans be conducted annually" and that plans "should be exercised no less than once every two years". [28] Public Safety Canada's guide for SDAs also recommends that "each SDA conduct a periodic review of their BCP program including risks, BIA, plans, training/awareness, and testing. As a rule, a review of the program should be conducted every two years, or after the plan was exercised or activated." [29]

None of the departments included in this audit have fully complied with the previously mentioned requirements and recommended practices in effect during the audit period. Specifically, the majority of large and small departments did not demonstrate having put in place BCP monitoring and reporting frameworks to ensure their compliance with the government's security policy framework and the overall effectiveness of their BCP programs. Half of the large departments also have not proactively tested their business continuity plans

sampled as part of the audit. For those that did, none demonstrated having conducted full-scale [30] tests, and the testing conducted was either limited to table top exercises, call-out exercises [31], or was limited to certain areas (for example, specific services, branches, directorates, etc.). The majority of small departments did not demonstrate having tested the business continuity plans sampled as part of the audit. Moreover, none of the departments demonstrated having adopted formal testing programs that encompass regular testing and validation of all business continuity plans in accordance with the government's policy requirements and recommended practices.

Departmental representatives from both large and small departments provided various explanations regarding the lack of monitoring. Several representatives mentioned relying on MAF assessments conducted by the Secretariat to assess the compliance of their departmental BCP programs with the government's security policy framework. Some representatives also noted that the guidance issued by the Secretariat and Public Safety Canada regarding monitoring of departmental BCP programs was too broad and/or unclear. Others mentioned having limited resources to dedicate in this area.

Regular formal monitoring and reporting on the overall compliance as well as effectiveness of departmental BCP programs would enable departments to proactively identify and address any existing gaps in order to enhance their resilience to events that disrupt normal business operations. As a key component of such monitoring and reporting frameworks, the periodic testing of business continuity plans would provide departments with practical assurance of the likelihood that these plans will work when faced with such disruptions.

Governance frameworks at the department level

Elements of departmental BCP governance frameworks such as the following were generally in place in all departments: governance committees, formal policies (in large departments), DSOs, and BCP Coordinators.

Both large and small departments could improve their BCP governance frameworks through more active involvement from the governance committees in place; better communication of roles and responsibilities to employees; and the implementation of formal monitoring and reporting frameworks (including formal exercise programs).

In large departments, there is also an opportunity to ensure that BCP program policies are updated in a timely manner and further formalize the reporting relationship between the DSOs and deputy heads (or executive committees).

Finally, there is an opportunity in small departments to put in place formally approved BCP program policies.

Recommendations – governance at the departmental level

6. Departments should ensure that up-to-date BCP program policies are in place and align with the government's security policy framework.
7. Departments should ensure that BCP roles, responsibilities, and reporting relationships are formally communicated to all employees involved in the departmental BCP process.
8. Departments should ensure that governance committees are actively supporting BCP by meeting regularly and systematically following-up on initiatives in this regard.
9. Departments should establish formal BCP monitoring and reporting frameworks, including testing programs, to ensure compliance with the government's security policy framework as well as the overall effectiveness of BCP programs.

Finding 3: departmental BCP processes

As part of baseline security requirements, all departments must have business continuity plans in place to provide for the continuity of government operations, regardless of whether they deliver critical services or not. [32] Conducting a BIA is a fundamental starting point in the process for developing such plans. The Operational Security Standard – Business Continuity Planning (BCP) Program outlines various other activities that must be conducted as part of this process, including requirements for the content of BIAs and business continuity plans. [33]

The audit assessed a risk-based [34] sample of BIAs and departmental business continuity plans to determine the extent to which departments complied with these requirements.

The majority of departments conducted BIAs. However, they generally do not fully meet most of the baseline requirements in this regard.

Departments were expected to have conducted BIAs to identify and prioritize all the services they delivered based on criticality (for example, from a departmental perspective [35] and from a government-wide perspective [36]). BIAs are foundational to the BCP process because BIAs provide the basic information needed by departments to strategically focus their efforts and limited resources in the areas that matter most for the continuity of their operations.

The Operational Security Standard – Business Continuity Planning (BCP) Program requires that departments follow the following steps when conducting BIAs:

a. determine the nature of the department's business (e.g. role, mandate) and the services it must deliver. Internal and external functions on which services depend must also be identified
b. determine the direct and indirect impacts of disruptions on the department, including the quantitative and qualitative effects
c. assess services to determine which are likely to cause high degree of injury to Canadians and the government, if disrupted

d. identify and prioritize critical services and list the resources (personnel, contractors, suppliers, information, systems and other assets) that support them directly or indirectly, within or outside the department. Priority is assigned based on the maximum allowable downtime [37] and the minimum service level [38] required before high degree of injury [39] will result. Services that must always be available, for which a disruption is not acceptable and immediate recovery is essential, are ranked at the top
e. obtain senior management approval of the results of the business impact analysis before proceeding with the development of continuity plans

Although BIAs were completed in the majority of departments, this was not the case in two large departments and one small department.

Moreover, both large and small departments generally did not fully comply with most of the previously listed requirements prescribed for BIAs under the Operational Security Standard – Business Continuity Planning (BCP) Program.

In this regard, the opportunities for improvements identified by the audit were most significant in the following areas: assessment of services to determine which are likely to cause high degree of injury to Canadians and the government; prioritization of services based on their maximum allowable downtimes and minimum service levels; senior management approval of BIAs; and, the identification of internal and external dependencies (for example, with other functions, resources, departments, etc.) relied upon for service delivery. [40]

Conducting comprehensive BIAs in alignment with all baseline requirements would help to enhance the quality of the information available for BCP in departments. In turn, this could help departments increase the overall effectiveness of their BCP program.

The majority of departments had business continuity plans for all services sampled. However, several opportunities for improvement were noted regarding their content and the processes carried out for developing these plans.

Business continuity plans are the main outputs of the BCP process and essentially provide a blueprint for the actions that will need to be undertaken in the event of a disruption to normal business operations. More specifically, they contain pre-established and agreed-upon procedures, including all the relevant information for enabling the continuity and subsequent recovery of departmental business operations impacted by disruptions.

Based on the results on their BIAs, departments are required, under the Operational Security Standard – Business Continuity Planning (BCP) Program, to undertake the following activities as part of the process for developing their business continuity plans:

a. development of recovery options, from which to determine a recovery strategy for each critical service
b. assessment of each option in terms of possible disruption, impacts on the department, benefits, risks, feasibility, and cost in order to select the most appropriate strategy

c. obtaining senior management approval to support and fund selected strategies
d. development of business continuity plans identifying:
    i. critical services, information assets, and dependencies identified in the business impact analysis
    ii. approved recovery strategies
    iii. measures to deal with the impacts and effects of disruptions on the department
    iv. response and recovery teams, including the membership and contact information
    v. roles, responsibilities and tasks of the teams including internal and external stakeholders
    vi. resources and procedures for recovery
    vii. coordination mechanisms and procedures
    viii. communications strategies
e. obtaining senior management approval of developed plans

Departments generally had business continuity plans in place covering all of the services sampled. More specifically, all of the small departments had such plans for each service sampled, but this was not the case in some of the large departments.

Overall, the business continuity plans examined in small departments mostly contained all of the basic information required under the Operational Security Standard – Business Continuity Planning (BCP) Program (section 3.3 d.). However, the opposite was observed in the large departments. Opportunities for improvements in both large and small departments were most significant with respect to the identification of internal and external interdependencies relied upon and to the identification of resources as well as procedures for recovery. [41] In large departments, there were also more significant opportunities for improvements regarding the identification of the following elements: measures to deal with the impacts and effects of disruptions; roles, responsibilities, and tasks of teams including internal and external stakeholders; and, communications strategies. [42]

As for departmental BCP processes, departments generally have not followed most of the steps prescribed under the Operational Security Standard – Business Continuity Planning (BCP) Program (section 3.3 a to e) for developing all the business continuity plans sampled. Opportunities for improvements were more significant in developing and in assessing recovery options before selecting recovery strategies. [43] In large departments, more significant opportunities for improvements were also noted regarding the approval of business continuity plans. [44]

By ensuring that BIAs as well as business continuity plans are developed in full alignment with baseline requirements and contain all the information required, departments would be in a better position to ensure the continuity of their operations in the event of a disruption. Addressing all interdependencies between departments will also be key for ensuring the effectiveness of business continuity plans, given the government's growing adoption of shared service delivery models.

Departmental BCP processes:

The majority of departments have conducted BIAs and had business continuity plans in place for the services sampled.

However, departments generally have not fully met most of the baseline requirements for BIAs. Several opportunities for improvement were also noted regarding the content of the departmental business continuity plans examined and the processes followed to develop these plans.

Recommendations – Departmental BCP processes

10. Departments should conduct BIAs that cover all services/programs in alignment with all baseline requirements.
11. Departments should ensure that business continuity plans are in place and that they have been developed in accordance with baseline requirements.

Conclusion

Overall, the audit noted a significant need for improvements to the government-wide and departmental governance frameworks as well as to the BCP processes in place within departments.

At the government-wide level, opportunities for improvements to BCP governance were noted with respect to the: updating and accessibility of policy instruments; the support from senior interdepartmental governance committees; the need for strategic planning; the approach for the identification and prioritization of critical services; and, the monitoring and reporting frameworks.

Within departments, there is also a need to improve governance over BCP through more active support from governance committees, better communication of roles and responsibilities, and stronger monitoring and reporting frameworks (including exercise programs to test business continuity plans).

Finally, the alignment of departmental BIA and BCP processes with baseline requirements also needs improvement.

Management response

The findings and recommendations of this audit were presented to the Secretariat, Public Safety Canada and the Privy Council Office along with the eight large departments as well as seven small departments that participated in this audit.

Management has agreed with the findings included in this report and will take action to address all applicable recommendations.

Appendix A: applicable policies, directives, standards, guidance, and best practices

Policies, Directives, Standards, Guidance, and Best Practices	Description
Policy on Government Security Effective date: July 1, 2009 Last updated on: April 1 2012	The objectives of this policy are to ensure that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management.
Directive on Departmental Security Management Effective date: July 1, 2009	The objective of this directive is to achieve efficient, effective and accountable management of security within departments.
Operational Security Standard – Business Continuity Planning (BCP) Program Last updated on: March 23, 2004	This standard defines baseline security requirements for establishing BCP programs that federal departments must fulfill to ensure the continued delivery of government services.
Federal Policy for Emergency Management Last updated on: January 1, 2016	The objective of this policy is to promote an integrated and resilient whole-of-government approach to emergency management planning, which includes better prevention/mitigation of, preparedness for, response to, and recovery from emergencies.

Policies, Directives, Standards, Guidance, and Best Practices	Description
Technical guidance issued by Public Safety Canada	• An Emergency Management Framework for Canada Second Edition (last modified on June 17, 2016) • Federal Emergency Response Plan January 2011 • A Guide to Business Continuity Planning (last updated: March 27, 2014): provides a summary and general guidelines for BCP. • Business Continuity Planning Program Technical Documentation • Short Guide to Business Continuity Planning in the Government of Canada (issued on October 2006) • A Guide for Developing a Business Continuity Management Program for Small Departments and Agencies (issued in April 2016, after the audit period)
Disaster Recovery Institute's International Professional Practices Framework for Continuity Practitioners (DRI PPF) Published in 2013	The Disaster Recovery Institute is the leading organization providing internationally recognized education and certification to business continuity professionals. The Professional Practices Framework is a body of knowledge designed to assist the entity in the development and implementation of a BCP program.

Appendix B: departments included in the audit

Lead Security Agencies (including policy centre), large and small departments were selected for this audit through both a risk assessment and a self-identification exercise conducted as part of the Office of the Comptroller General's risk-based audit planning.

The following Lead Security Agencies (including policy centre) were selected for inclusion in the audit:

1. Treasury Board of Canada Secretariat (the Secretariat) – Central Agency/Policy Centre
2. Public Safety Canada (PS)
3. Privy Council Office (PCO)

The following large departments were selected for inclusion in the audit (an asterisk (*) denotes a Shared Services Canada partner organization):

1. Agriculture and Agri-Food Canada* (AAFC)

2. Canada Border Services Agency* (CBSA)
3. Environment and Climate Change Canada* (ECCC)
4. Global Affairs Canada* (GAC)
5. Public Services and Procurement Canada* (PSPC)
6. Royal Canadian Mounted Police* (RCMP)
7. Shared Services Canada (SSC)
8. Transport Canada* (TC)

The following small departments were selected for inclusion in the audit:

1. Canadian Environmental Assessment Agency (CEAA)
2. Canadian Nuclear Safety Commission* (CNSC)
3. Canadian Transportation Agency (CTA)
4. Courts Administration Service (CAS)
5. Parole Board of Canada (PBC)
6. Transportation Safety Board of Canada (TSB)
7. Western Economic Diversification Canada* (WD)

Note: Shared service providers / Enterprise Service Organizations: SSC and PSPC.

Appendix C: lines of enquiry and audit criteria

The audit criteria are presented in the table below, by audit line of enquiry.

Line of Enquiry	Criteria	Source
1 – Government-wide governance Framework. A government-wide governance framework is in place for the management of BCP government-wide.	1.1 Governance structures that actively support government-wide BCP are in place and, their roles as well as responsibilities have been documented, approved, and communicated to all stakeholders.	PGS [1] (3.4, 6.11, Appendix B) DRI-PPF [2] (1.2.d, 1.2.f, 1.2.h, 1.2.i, 1.3.g, 1.3.h)
	1.2 A government-wide policy framework defining roles, responsibilities, expectations and best practices for BCP is in place and up-to-date to reflect the operating environment.	EMA [3] 4.1 (a), (b), (m), (n), (o), 6.2 (c) PGS (6.2.1, Appendix B)
	1.3 A government-wide BCP strategy and systematic approach for [This information has been withheld]	[This information has been withheld] [4] [5]

Line of Enquiry	Criteria	Source
	1.4 Interdepartmental coordination and collaboration processes are in place to integrate BCP and recovery activities across government.	EMA 3, 4.1 (e), (n), (o), (r) PGS (Appendix B) OSS-BCP (3.1, 2h) DRI-PPF (2.5.b, f, 3.5.b, 6.1.a(i), b(i))
2 – Departmental Governance Framework. Departmental governance frameworks are in place for the management of departmental BCP.	2.1 Departmental governance structures that actively support business continuity planning are in place and, their roles as well as responsibilities have been documented, approved, and communicated to all stakeholders.	PGS (6.1.1) OSS-BCP (3.1) DRI-PPF (Program Initiation and Management)
	2.2 A departmental policy framework defining roles, responsibilities, and expectations for BCP is in place.	PGS (3.6, 6.1.1.b, 6.2.3) OSS-BCP (3.1) Public Safety Canada A Guide on Business Continuity Planning Guideline on Service Agreements: Essential Elements (Section 1) DRII (PP6, PP8)
	2.3 A department-wide systematic approach to identify and prioritize departmental critical services is in place.	PGS (3.3, 6.1.1.c, 6.1.4, 6.3) OSS-BCP (3.1) DDSM (6.1.1.4)

Line of Enquiry	Criteria	Source
	3.1 Departments have conducted Business Impact Analysis (BIA).	OSS-BCP (3.2) DDSM (Appendix C, Emergency and business continuity planning) DRI-PPF (3)
	3.2 Departments developed recovery strategies for the critical services identified in their BIA(s) which take into account interdependencies with other departments.	OSS-BCP (3.3 a-c) DDSM (Appendix C, Emergency and business continuity planning) DRI-PPF (4)
	3.3 Departments developed business continuity plans to ensure the continuity of their critical services and critical support services.	EMA 6.1(a), 6.2(c) OSS-BCP (3.1 1h; 3.3 d-e) DDSM (Appendix C, Emergency and business continuity planning) DRI-PPF (4, 6.1b)
	3.4 Departments coordinate with Critical Support Service Providers and other key internal stakeholders when developing, testing and updating their BCP to ensure integration between all parties.	OSS-BCP (3.1 1h; 3.3 d.vii)

Line of Enquiry	Criteria	Source
	3.5 Departments ensure that sufficient and relevant training as well as tools are provided to enable BCP and recovery activities.	EMA 6.1(c) PGS (3.3 , 3.5, Appendix B) OSS-BCP (3.1, 3.3.g) DRI-PPF (6.2(iv-v), 7, 7.4.d(i))
	3.6 Departments ensure that their business continuity plans are periodically tested, updated and reflect interdependencies with other stakeholders.	EMA 6.1(b), (c) OSS-BCP (3.4.a,c) DDSM (Appendix C, Emergency and business continuity planning) DRI-PPF (8.1, 8.2)
4 – Monitoring. Government-wide and departmental monitoring processes are in place for the oversight of BCP readiness.	4.1 Departments monitor and report on the effectiveness of their BCP.	PGS (6.1.1c) DDSM (6.1.9, 6.2.1)
	4.2 Departments monitor their compliance with BCP related requirements in the TB Policy on Government Security and inform the Secretariat of any gaps identified.	PGS (6.3) OSS-BCP (3.4.d)
	4.3 LSAs regularly monitor and report on the government's readiness for disruption events.	EMA 4(1)(c) (n) Federal Policy for Emergency Management, 9.2 PGS (6.3, and Appendix B)

Line of Enquiry	Criteria	Source
	4.4 The Secretariat monitors and reports on the effectiveness and compliance with BCP related requirements in the TB policy framework.	PGS (6.3, Government-wide and Appendix B)

1	Policy on Government Security
2	Disaster Recovery Institute's International Professional Practices Framework
3	Emergency Management Act
4	[This information has been withheld]
5	[This information has been withheld]

Appendix D: recommendations by department and risk ranking

The following table presents the departments to which the audit recommendations apply and assigns a risk ranking of high, medium, or low to each recommendation. The determination of risk rankings was based on the relative priorities of the recommendations and the extent to which the recommendations indicate non-compliance with Treasury Board policies. The full names of the departments are provided in Appendix B.

Recommendations	Departments To Which This Recommendation Applies [1]	Priority Level [2]

Recommendations	Departments To Which This Recommendation Applies [1]	Priority Level [2]
1. Public Safety Canada and the Secretariat should ensure that appropriate work plans to expedite the renewal of policy instruments that support BCP are in place and regularly monitored. In doing so, the Secretariat should also determine how to strengthen the linkages to Public Safety Canada's technical guidance on BCP within the renewed Treasury Board security policy framework. (Applies to opportunities for improvement identified under audit criterion: 1.2)	PS, and the Secretariat	High
2. Public Safety Canada should ensure that its technical guidance on BCP is communicated and made readily accessible to all departments. (Applies to opportunities for improvement identified audit criterion: 1.2)	PS	High
3. Public Safety Canada and the Secretariat should periodically raise the profile of BCP in the agendas of interdepartmental senior management committee meetings related to security and emergency management. Representation of small departments at these committees should also be strengthened (Applies to opportunities for improvement identified under audit sub-criteria: 1.1.1 to 1.1.3, 1.3.1, 1.3.2 and 4.3)	PS, and the Secretariat	High
4. Public Safety Canada should, in consultation with the Secretariat, develop and implement a formal monitoring and reporting framework for periodically assessing the business continuity plans of other departments. (Applies to opportunities for improvement identified under audit criterion: 4.3)	PS	High

Recommendations	Departments To Which This Recommendation Applies [1]	Priority Level [2]
5. The Secretariat, with Public Safety Canada and the Privy Council Office, should establish a results-based government-wide strategy to strengthen the continuity of government operations and support federal departments in strengthening their BCP programs. The strategy should: a. address the specific needs of departments (for example, via practical hands-on training, tools, technical guidance, capacity development activities, targeted support where required, etc.) b. include the development of a proactive approach for enabling departments to provide timely and accurate BCP information, [This information has been withheld] c. be developed in consultation with the relevant senior interdepartmental security and emergency management committees, and specify the contributions of these committees for strengthening BCP government-wide d. be regularly monitored by the Secretariat, with Public Safety Canada, to help ensure the achievement of targeted results e. take into consideration the results of all government-wide monitoring activities relating to BCP (for example, MAF assessments conducted by the Secretariat, evaluations of departmental business continuity plans conducted by Public Safety Canada, maturity assessments, etc.) **(Applies to opportunities for improvement identified in audit sub-criteria: 1.3.1 and 1.3.2)**	PS, the Secretariat, PCO	High
6. Departments should ensure that up-to-date BCP program policies are in place and align with the government's security policy framework. **(Applies to opportunities for improvement identified under audit sub-criterion: 2.2.1, 2.2.2, and 2.2.3)**	AAFC, ECCC, RCMP, CTA, CEAA, PBC, WD, TSB	Medium

Recommendations	Departments To Which This Recommendation Applies [1]	Priority Level [2]
7. Departments should ensure that BCP roles, responsibilities, and reporting relationships are formally communicated to all employees involved in the departmental BCP process. (Applies to opportunities for improvement identified under audit sub-criterion: 2.1.3)	GAC, ECCC, TC, PSPC, SSC, and all small departments identified in Appendix B	High
8. Departments should ensure that governance committees are actively supporting BCP by meeting regularly and systematically following-up on initiatives in this regard. (Applies to opportunities for improvement identified under audit sub-criterion: 2.1.1, 2.1.2, and 2.1.4)	AAFC, GAC, PSPC, SSC, CNSC, CAS, CEAA, PBC, WD, TSB	High
9. Departments should establish formal BCP monitoring and reporting frameworks (including testing programs) to ensure compliance with the government's security policy framework as well as the overall effectiveness of BCP programs. (Applies to opportunities for improvement identified under audit sub-criteria: 3.6.1, 3.6.2, 4.1, and 4.2)	All large and small departments identified in Appendix B	High
10. Departments should conduct BIAs that cover all services/programs in alignment with all baseline requirements. (Applies to opportunities for improvement identified under audit sub-criteria: 2.3.1, 2.3.2, and 3.1)	AAFC, CBSA, GAC, PSPC, RCMP, SSC, TC, CEAA, CNSC, CTA, CAS, PBC, TSB, WD	High
11. Departments should ensure that business continuity plans are in place and that they have been developed in accordance with baseline requirements. (Applies to opportunities for improvement identified audit criteria 3.2 and 3.3)	All large and small departments identified in Appendix B	High

Recommendations	Departments To Which This Recommendation Applies [1]	Priority Level [2]

[1] Recommendations were made to address horizontal findings (at the government-wide level). As such, when directed at more than one department, recommendations may apply entirely or only partially to the individual departments listed in this Appendix; depending on the specific findings observed in each department.

[2] Priority levels were assigned based on risks from a government-wide perspective. Given that the findings in each department varied, the level of risk from a departmental perspective may vary.

Appendix E: additional background on emergency management

Emergency management in federal, provincial, and territorial governments adopts a comprehensive all-hazards approach to coordinating and integrating the prevention and mitigation, preparedness, response and recovery activities to maximize the safety of Canadians. More specifically, this approach includes the following activities: [45]

- **prevention and mitigation:** eliminates or reduces the risks of disasters. Prevention/mitigation includes structural measures (such as construction of floodways and dykes) and non-structural measures (such as building codes, land-use planning, and insurance incentives).
- **preparedness:** aims at being ready to respond to a disaster and to manage its consequences through measures taken prior to an event (for example, emergency response plans, mutual assistance agreements, resource inventories and training, equipment and exercise programs, etc.).
- **response:** consists in taking action during, immediately before, or immediately after a disaster to manage its consequences (e.g. emergency public communication, search and rescue, emergency medical assistance, evacuation, etc.).
- **recovery:** consists in repairing or restoring conditions to an acceptable level through measures taken after a disaster (such as return of evacuees, trauma counseling, reconstruction, etc.).

BCP is a component of emergency management since it supports the preparedness, response, and recovery activities described above. Notwithstanding the specific origin and magnitude of an emergency or event, it is important to note that business continuity plans may be implemented in response to localized events, or in the context a larger government-wide response.

Appendix F: roles and responsibilities of the main lead security agencies and central agency

Main departments	Summary of roles and responsibilities for supporting government-wide BCP

Main departments	Summary of roles and responsibilities for supporting government-wide BCP
Treasury Board and the Secretariat. (Central Agency / Policy Centre)	The roles and responsibilities of the Treasury Board and the Secretariat are detailed in the Financial Administration Act and in the Treasury Board Policy on Government Security. The main responsibilities of the Treasury Board and the Secretariat for supporting government-wide BCP are summarized below: • Under section 7 of the Financial Administration Act, Treasury Board has the authority to issue a security policy and directives for the Government of Canada. In turn, Treasury Board delegated to the President of the Treasury Board the authority to amend such directives as needed, including the authority to issue as well as amend related standards in the area of BCP. As the administrative arm of the Treasury Board reporting to its President, the Secretariat is the central agency responsible for developing and maintaining government-wide management policy instruments in this area • Under the Policy on Government Security(Appendix B), the Secretariat is responsible for: ◦ establishing and maintaining interdepartmental governance to oversee a whole-of-government approach to security ◦ exercising strategic oversight, providing leadership, and establishing priorities related to government security ◦ ensuring that periodic reviews are conducted to assess the effectiveness of its security support services to ensure they continue to meet the needs of departments and the government as a whole • The Secretariat is responsible for monitoring government-wide compliance with the Treasury Board security policy suite and the achievement of its expected results. The Secretariat is also expected to have reviewed and reported to the Treasury Board on the effectiveness and implementation of this policy suite at the five-year mark from the effective date of the Policy on Government Security (that is, by July 2014)

Main departments	Summary of roles and responsibilities for supporting government-wide BCP
Public Safety Canada. (lead security agency and federal coordinating department for emergency management in Canada)	The roles and responsibilities of Public Safety Canada are detailed in the Emergency Management Act, in the Treasury Board Policy on Government Security, and in the Federal Policy for Emergency Management. The main responsibilities of Public Safety Canada relevant to BCP are summarized below: • The Emergency Management Act assigns Public Safety Canada the responsibility for: ◦ exercising leadership and acting as the federal coordinating department in matters relating to emergency management in Canada. Included in this broad responsibility are the authority to establish policies respecting the preparation, maintenance, testing, and implementation by a government institution of emergency management plans, as well as the authority to establish policies and programs respecting emergency management. According to the Emergency Management Act, the term "emergency management plans" encompasses programs, arrangements, or other measures providing for the continuity of operations of government institutions ◦ "analyzing and evaluating emergency management plans prepared by government institutions" including business continuity plans ◦ conducting exercises related to emergency management • In terms of reporting, there is a requirement in the Federal Policy for Emergency Management for Public Safety Canada to "report every two years to the Deputy Ministers' Committee responsible for emergency management issues on government-wide readiness of the federal emergency management system, based on the information reported by federal institutions and work undertaken directly by Public Safety Canada" • Under the Policy on Government Security, Public Safety Canada is responsible for ensuring that "periodic reviews are conducted to assess the effectiveness of its security support services to ensure they continue to meet the needs of departments and the government as a whole"

Main departments	Summary of roles and responsibilities for supporting government-wide BCP
Privy Council Office. (lead security agency)	The Privy Council Office (PCO) is identified as a lead security agency in Appendix B of the Policy on Government Security. PCO advises and supports the Prime Minister and Cabinet on national security matters and coordinates the related activities of departments and agencies. Under the Policy on Government Security, PCO is responsible for: • providing government-wide policy direction on national security and intelligence priorities • advising departments on strategies, mechanisms and activities required to develop, implement, evaluate and improve a fully integrated security system in the GC in support of national security objectives • providing direction to Public Safety Canada to help resolve government security incidents and events that may affect national security • providing direction and advice to departments and agencies on implementing security readiness levels in emergency and increased threat situations • supporting the Prime Minister in establishing candidates' fitness for office for public office positions and conducting security clearances for deputy heads • providing direction and advice to departments and agencies on the level of security support to be provided to ministers, secretaries of State and parliamentary secretaries; and • establishing government policy on the security of Cabinet Confidences (Confidences of the Queen's Privy Council for Canada) and of records administered under the Cabinet Papers System and coordinating the investigation into unauthorized disclosure or other compromise of those documents

Footnotes

1 See Appendix C for the specific aspects of governance and BCP processes examined as part of this audit.

2 IT Continuity Planning (also known as disaster recovery planning) deals with recovering IT assets after a disastrous interruption (Public Safety Canada, A Guide to Business Continuity Planning).

3 The Emergency Management Vocabulary Terminology Bulletin 281 defines continuity of constitutional government as the process of establishing defined plans and procedures that allow the three branches (executive, legislative, and judicial) of the constitutional Government of Canada to continue conducting essential operations in case of an emergency or a disaster in the National Capital Region.

4 The Global Risks Report 2017, 12th edition (PDF, 7.8 MB), World Economic Forum, Figure 2, Top 5 Global Risks in Terms of Likelihood, page 4.

5 Treasury Board Policy on Government Security, Appendix A – Glossary, "critical service".

6 Resilience means: "The ability to quickly recover from disruptions and maintain service delivery" (Business Continuity Planning Program Technical documentation, Public Safety Canada).

7 All-hazard approach is defined as "an emergency management approach that recognizes that the actions required to mitigate the effects of emergencies are essentially the same, irrespective of the nature of the incident, thereby permitting an optimization of planning, response and support resources" (Emergency Management Vocabulary, Terminology Bulletin 281).

8 Operational Security - Business Continuity Planning (BCP) Program, Standard, Section 3

9 BIAs are conducted to assess the impacts of disruptions on the department and to identify and prioritize critical services and associated assets. A BIA involves the steps outlined in section 3.2 of the Operational Security - Business Continuity Planning (BCP) Program, Standard.

10 Business continuity plans include information such as: recovery strategies; communication strategies; roles, responsibilities and tasks of response as well as recovery teams including internal and external stakeholders, etc. For further details, see section 3.3 of the Operational Security - Business Continuity Planning (BCP) Program, Standard.

11 See Appendix C for the specific aspects of governance and BCP processes examined as part of this audit.

12 Risk-based sampling (or justified sampling) is defined by the Institute of Internal Auditors (IIA) as a non-random sample selected using auditor judgement based on a pre-determined set of risk attributes (IIA Practice Advisory 2320-3).

13 IT continuity planning (also known as disaster recovery planning) deals with recovering IT assets after a disastrous interruption. (Public Safety Canada, A Guide to Business Continuity Planning)

14 The Emergency Management Vocabulary Terminology Bulletin 281 defines continuity of constitutional government as the process of establishing defined plans and procedures that allow the three branches (executive, legislative, and judicial) of the constitutional Government of Canada to continue conducting essential operations in case of an emergency or a disaster in the National Capital Region.

15 BCP is considered a basic security requirement (TBS, Policy on Government Security, 3.3; and, TBS OSS-BCP, Preamble).

16 This approach is described under section 3.2 of the Operational Security Standard – Business Continuity Planning (BCP) program.

17 According to the FERP, "All-hazard risk approach is an approach that recognizes that the actions required to mitigate the effects of emergencies are essentially the same, irrespective of the nature of the event, thereby permitting an optimization of scarce planning, response and support resources. The intention of all-hazards generic emergency planning is to employ generic methodologies, modified as necessary by particular circumstances. All-hazards incorporates natural and man-made hazards threats including traditional emergency management events such as flooding and industrial accidents, as well as national security events such as acts of terrorism, and cyber events" (FERP, Annex D – Glossary of terms and definitions)

18 An overview of this structure is described in section 2.3 of the FERP.

19 [This information has been withheld]

20 For the purpose of this audit, "functionally responsible" (functional reporting relationship) means that the DSO has a formal duty to regularly report to the deputy head or executive committee on the management of the departmental security program (for example, status, compliance, performance, etc.).

21 The BCP Coordinator is responsible for establishing and managing the departmental BCP program on a day-to-day basis. For further details on the responsibilities of the BCP Coordinator, see section 3.1 of the Operational Security Standard – Business Continuity Planning (BCP) Program.

22 For the purpose of this audit, this duty for the BCP Coordinator to inform the DSO throughout the BCP process was deemed as a functional reporting relationship.

23 For the purpose of this audit, "functional managers" refers to any individual within a department who has been assigned the primary responsibility for developing and maintaining the business continuity plans for the sections/directorate under his/her direct supervisory authority (for example, service delivery managers).

24 Operational Security Standard – Business Continuity Planning (BCP) Program, Section 3.4 c.

25 A Guide to Business Continuity Planning, Quality assurance techniques, internal review.

26 "An orientation/walk-through session is the most basic type of exercise. The objective of the exercise is to walk employees through the steps of the plan in order to ensure they know their respective roles and responsibilities in the event of an emergency" (A Guide for Developing a Business Continuity Management Program for Small Departments and Agencies (SDAs), section 4).

27 "Tabletop exercises are discussion-based sessions where certain departmental representatives meet in an informal setting to discuss their roles and responsibilities during an emergency and their responses to a particular emergency scenario." (A Guide for Developing a Business Continuity Management Program for Small Departments and Agencies (SDAs), Annex C, section 5).

28 A Guide for Developing a Business Continuity Management Program for Small Departments and Agencies (SDAs), section 7.2

29 A Guide for Developing a Business Continuity Management Program for Small Departments and Agencies (SDAs), section, 7.3

30 Full-scale tests (such as drills) are exercises that simulate a full deployment to the alternate site and evaluates the entire business continuity plan or plans with all the necessary resources, personnel or equipment. All critical services are exercised. (Short Guide to Business continuity planning in the Government of Canada, Public Safety Canada, October 2006).

31 Call-out exercises are conducted to validate that the contact information included in the plans is correct. In addition, call-out exercises test the speed at which information can be disseminated via the department's hierarchy (A Guide for Developing a Business Continuity Management Program for Small Departments and Agencies (SDAs), Annex C, section 5).

32 See the following: Emergency Management Act, Section 6(2) (c); Operational Security Standard – Business Continuity Planning (BCP) Program, Section 1; and, the joint interpretation issued by Public Safety Canada and the Secretariat on January 15th, 2016.

33 Operational Security Standard – Business Continuity Planning (BCP) Program, Sections 3.2 and 3.3 (a-e).

34 Risk-based sampling (or justified sampling) is defined by the Institute of Internal Auditors (IIA) as a non-random sample selected using the auditor judgement based on a pre-determined set of risk attributes (IIA Practice Advisory 2320-3).

35 Refers to the services that are critical to the mandate of the department (mission critical).

36 Refers to critical services as defined under the Treasury Board Policy on Government Security.

37 Maximum allowable downtime refers to the longest period of time for which a service can be unavailable or degraded before a high degree of injury results (Operational Security Standard – Business Continuity Planning (BCP) Program, Appendix 1).

38 Minimum service level refers to the level of service delivery which is essential to avoid a high degree of injury; is maintained until full recovery is achieved (Operational Security Standard – Business Continuity Planning (BCP) Program, Appendix 1).

39 High degree of injury means: severe harm related to the provision of sustenance (e.g., food, water, shelter, energy), public order, emergency care and response, a life-sustaining environment, vital communications and transportation, fundamental economic services, continuity of government, territorial integrity and sovereignty (Operational Security Standard – Business Continuity Planning (BCP) Program).

40 Operational Security Standard – Business Continuity Planning (BCP) Program, section 3.2 c, d, and e.

41 Operational Security Standard – Business Continuity Planning (BCP) Program, section 3.3 d.i & vi

42 Operational Security Standard – Business Continuity Planning (BCP) Program, section 3.3 d.iii, v, and viii

43 Operational Security Standard – Business Continuity Planning (BCP) Program, section 3.3 a-c

44 Operational Security Standard – Business Continuity Planning (BCP) Program, section 3.3 e

45 Emergency Management Framework for Canada Second Edition, Emergency management components

© Her Majesty the Queen in Right of Canada, represented by the President of the Treasury Board, 2018,
ISBN: 978-0-660-27228-3

Date modified:

2018-08-17